REMARKS

In response to the above-identified Office Action, Applicants amend the application and seeks reconsideration thereof. In this response, Applicants amend claims 1, 11, and 18. Applicants do not cancel any claims or add any new claims. Accordingly, claims 1-26 are pending.

I. Claims Rejected Under 35 U.S.C. § 103(a)

Claims 1-9, 11-14, 16, 18-21, 23-24, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,748,539 issued to Lotspiech ("Lotspiech") in view of U.S. Pre-Grant Patent Application No. 2001/0032088 applied for by Utsumi et al. ("Utsumi"). Applicants respectfully traverse the rejection.

To establish a *prima facie* case of obviousness, the Examiner must show the cited references, combined, teach or suggest each of the elements of a claim. Amended claim 1 recites the element "an encryption subsystem housed in a storage device to encrypt data ... using an encryption bus key prior to transmitting the encrypted data via a data bus, wherein the data bus connects to a destination in which the encrypted data is to be decrypted and said encryption bus key is derived based on [1] a portion of the key distribution data block, [2] a device key assigned to said encryption subsystem and [3] the nonce received over the data bus from the number generator." (Emphasis added). Applicants submit that Lotspiech at least does not teach or suggest these elements.

Applicants submit that the communication between Lotspiech's encryption module with the flash memory device (which carries the media ID and the encrypted contents) is not via the data bus as claimed. The communication is at most among the processing units within the kiosk. Communication links inside the kiosk do not connect to a destination of the encrypted data where the encrypted data is to be decrypted. Lotspiech does not disclose any data bus that connects the encryption subsystem to a destination in which the encrypted data is to be decrypted. Rather, a user of Lotspiech's system must carry the flash memory from the kiosk (where the content is encrypted) to the player (where the content is decrypted). Thus, Lotspiech does not teach or suggest each of the elements of Claim 1.

Moreover, Lotspiech's system is vulnerable to the replay attack against which the claimed system aims to protect. Applicants note that the Lotspiech's media ID (characterized as the nonce) is accessible for the entire duration of music rental because the ID is stored in a flash memory device (Fig. 1). The media ID is changed only after the flash memory is checked in at a kiosk where the music content is erased (col. 5, lines 21-27). Thus, after the rental music is encrypted and stored in the flash memory, a skilled artisan would be able to access the encrypted content, the media ID, and the media key block in the flash memory to make an unauthorized copy for replay. Storing the encrypted contents with the media ID used for the encryption on the same medium (the flash memory) makes it easier for the replay attack described in Applicants' specification at page 6, lines 1-9. Any host device having a device key would not be able to distinguish the unauthorized copy from a legitimate copy as both copies have the same information required for decryption and replay. Lotspiech's system is capable of protecting against replay attacks only after the media ID is altered and when the would-be attacker copies the contents back to the flash memory having the altered ID for replay (col. 5, lines 28-35).

In contrast, the claimed system is far superior in protecting against replay attacks. An attacker trying to intercept the encrypted data on the data bus would not be able to ascertain the nonce from which the encryption bus key is derived. Even if the attacker makes a copy of the encrypted content, a host would not be able to decrypt the data without knowing the nonce. Thus, Lotspiech does not teach or suggest each of the elements of claim 1.

The Examiner relies on Utsumi for disclosing the encryption subsystem housed within a storage device. Assuming for the sake of argument Utsumi discloses the storage device as claimed, Utsumi does not cure the defect of Lotspiech for failing to teach or suggest an encryption module that receives a nonce over the data bus and sends the encrypted data over the same data bus, wherein the data bus connects to a destination in which the encrypted data is to be decrypted. The concept of using a nonce received over the data bus is totally absent from Utsumi's disclosure. Thus, Lotspiech in view of Utsumi does not teach or suggest each of the elements of claim 1.

Moreover, Applicants respectfully submit that there is no motivation to combine these references. Utsumi is directed to a license devolution system in which user contents are transferred from a first storage medium to a second storage medium via a drive (Abstract, Figs. 1 and 2). Lotspiech is directed to a system for digitized content rental in which contents are transported between a kiosk and a player device via portable flash memory. Absent Applicants' claim that the encryption subsystem may be housed in a storage device, one would not have been motivated to combine Lotspiech with Utsumi as the two references teaches divergent means of transporting protected contents. Accordingly, this combination could only have been arrived at by hindsight. Hindsight is inappropriate as the Examiner is no doubt aware.

Analogous discussion applies to amended Claims 11 and 18. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 1, 11, and 18 are requested.

In regard to Claims 2-9, 12-14, 16, 19-21, 23-24, and 26, these claims depend from independent Claims 1, 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to Claims 1, 11, and 18, these claims are not obvious over Lotspiech in view of Utsumi. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 2-9, 12-14, 16, 19-21, 23-24, and 26 are requested.

Claims 10, 17, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and further in view of U.S. Patent No. 6,751,321 issued to Kato et al. ("Kato"). Applicants respectfully traverse this rejection.

Claims 10, 17, and 22 depend from Claims 2, 14, and 19 and incorporate the limitations thereof. Claims 2, 14, and 19 depend from independent Claims 1, 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to Claims 1, 11, and 18, Lotspiech and Utsumi do not teach or suggest each of the elements of these claims. Further, Kato does not cure the defects of Lotspiech and Utsumi. Nothing in Kato teaches or suggests an encryption module that receives a nonce over the data bus and sends the encrypted data over the same data bus, wherein the data bus connects to a destination in which the encrypted data is to be decrypted. Thus, Lotspiech in view of Utsumi and further in view of Kato does not teach or suggest each of the elements of Claims 10, 17, and 22.

Moreover, Claims 10, 17, and 22 recite the additional element that the number generator is a random number generator residing within the decrypting subsystem. From the cited passage at col. 5, lines 30-50, a skilled person would understand that each of the encryptor and the decryptor is locally coupled to a random number generator. The encryptor does not receive a random number from the decryption subsystem via the data bus 105, but rather uses a random number locally generated in the transmit device (Fig. 1). Thus, Lotspiech in view of Utsumi and further in view of Kato does not teach or suggest each of the elements of Claims 10, 17, and 22 for this additional reason.

Claims 10, 17, and 22 are also rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and further in view of the 1998 ACM article "A Practical Secure Physical Bit Generator" authored by Jakobsson et al. ("Jakobsson").

Jakobsson also does not cure the defects of Lotspiech and Utsumi. Nothing in Jakobsson teaches or suggests an encryption module that receives a nonce over the data bus and sends the encrypted data over the same data bus, wherein the data bus connects to a destination in which the encrypted data is to be decrypted. Moreover, Applicants submit that these dependent claims must be read together with their respective base claims which provide that the host device decrypts data. Jakobsson merely discloses using certain statistics of a computer hard drive (e.g., the access time) to derive randomness (Introduction). The Examiner has not identified and Applicants have been unable to discern any portion of Jakobsson that mentions data decryption. Thus, there is no motivation to combine Jakobsson with the other references because the concept of data protection is totally lacking in Jakobsson. Thus, Lotspiech in view of Utsumi and further in view of Jakobsson does not teach or suggest each of the elements of Claims 10, 17, and 22 for this additional reason. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 10, 17, and 22 are requested.

Claims 15 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and further in view of U.S. Patent Application No. 2002/0015494 applied for by Nagai, et al. ("Nagai"). Applicants respectfully traverse this rejection.

Claims 15 and 25 depend from independent Claims 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to Claims 11, and 18, Lotspiech and Utsumi do not teach or suggest each of the elements of these claims. Nagai does not cure the defects of Lotspiech and Utsumi. The Examiner relies on Nagai for teaching the descrambling. However, nothing in Nagai teaches or suggests all the elements recited in Claims 11 and 18. Thus, Lotspiech in view of Utsumi and further in view of Nagai does not teach or suggest each of the elements of Claims 15 and 25. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 15 and 25 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending, namely Claims 1-26 patentably define the subject invention over the prior art of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207 3800.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 7/20, 2005

Thomas Coester

Thomas M. Coester, Reg. No. 39,367

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF TRANSMISSION:

I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on July 20, 2005.

7-20-05

Lillian E. Rodriguez July 20, 2005